‘Chilling’: Some Smart Toys Can Collect Kids’ Iris Scans, Fingerprints, Vital Signs and More

Fri 5:31 pm +01:00, 8 Dec 2023

posted by pete fairhurst 2

“The annual “Trouble in Toyland” report, produced by the U.S. Public Interest Research Group (PIRG) and released before the holiday season, historically has focused on safety hazards found in traditional children’s toys.

But this year’s report highlights a new threat: “smart toys” that pose a privacy risk to children and families.

According to the 38th annual “Trouble in Toyland” report, released in mid-November, “Toys that spy on children are a growing threat.” The threats “stem from toys with microphones, cameras and trackers, as well as recalled toys, water beads, counterfeits and Meta Quest VR headsets.”

“The riskiest features of smart toys are those that can collect information, especially without our knowledge or used in a way that parents didn’t agree to,” said Teresa Murray, Consumer Watchdog at the U.S. PIRG Education Fund and author of the report. “It’s chilling to learn what some of these toys can do,” Murray said in a press release.

Murray told The Defender:

“This primarily means microphones, cameras, geolocators, Wi-Fi and Bluetooth capability or that connect to an app. We’re also watching for developments with artificial intelligence [AI] built into toys, although this isn’t happening much — yet.”

Smart toys include “stuffed animals that listen and talk, devices that learn their habits, games with online accounts, and smart speakers, watches, play kitchens and remote cars that connect to apps or other technology,” according to PIRG.

Dev Gowda, J.D., deputy director of Kids in Danger, told The Defender, “Parents and gift-givers should be concerned with toys that connect automatically to unsecured Wi-Fi networks or pair automatically with other devices through Bluetooth. Families may unknowingly share information through a toy’s microphone, camera, or video camera.”

According to the PIRG report, smart toys can pose the risk of data breaches, hacking, potential violations of children’s privacy laws such as the Children’s Online Privacy Protection Act of 1998 (COPPA), and exposure to “inappropriate or harmful material without proper filtering and parental controls.”

PIRG said:

“AI-enabled toys with a camera or microphone may be able to, for example, assess a child’s reactions using facial expressions or voice inflection. This may allow the toy to try and form a relationship with the child and gather and share information with others that could risk the child’s safety or privacy. …

SEARCH THE TAP

Search … Search

THE TAP BLOG

The blog that's fed by you, the readers. Please send in the news and stories that you think are of interest using the form below.

Your Name
Your Name

Your Email
Your Email

Post Title
Post Title

Moon Spelt Backwards
Antispam Question

Post Content
Post Content

Upload an Image
Please select your image(s) to upload.

Choose File No file chosen

Submit Post

TAP ARCHIVES

Select Month

LINKS AND ADS

Ecommerce-Help

Experts in Ecommerce and Shopping Carts

www.ecommerce-help.co.uk

Alternative View Media

Media group behind The Alternative View Conference

www.alternativeview.co.uk

THE TAP NEWSLETTER

"… Some [smart toys] can collect data on your child and transmit it off of the toy to a company's external servers. For example, some interactive dolls with conversation capabilities use microphones and Wi-Fi to transmit a child's words to speech recognition software maintained by the company."

California-based attorney Robert Barnes told The Defender Big Tech is "targeting kids built on monetizing their private information and manipulating them to achieve that objective. So-called smart toys can pose that same risk."

According to Research and Markets, the global market for smart toys grew to $16.65 billion in 2023, from $14.11 billion in 2022, and is expected to exceed $35 billion by 2027.

Austin, Texas-based technology attorney W. Scott McCollough told The Defender that smart toys are "another example of the alarming trend of corporate and government surveillance inside the home," that threatens privacy and liberty.

"Simply put, this cabal of private and public interests are voyeurs, noisy busybodies, but they also have coercive power," he said.

Along similar lines, California-based attorney Greg Glaser said "American moms and dads need to be careful, because tech companies are using toys to invade family privacy at home."

"Companies today see the real world as product research. Where there is data to be harvested and analyzed, there is danger," he said.

'We don't know' if they are recording or collecting data

According to PIRG, "An uncomfortable reality of smart toys" is that, "We don't know with certainty when our child plays with a connected toy that the company isn't recording us or collecting our data."

"Digging a little deeper, we're most concerned about smart toy features that parents can't easily control or turn off. For example, if there's a microphone in a stuffed animal, is there a 'wake word'? If so, that means the microphone is always on and listening for the wake word," Murray said.

"What else is it listening to or recording or sharing with goodness know who?" she asked.

As for where sensitive data may end up, Murray said, "The short answer is, it goes wherever the companies that collect it want it to go," adding that while the data collected "shouldn't be used in a way that isn't necessary for 'playtime,' or kept for longer than needed or that deviates from what parents agreed to. But it often is, unfortunately."

Murray said information collected by smart toys is valuable for toy manufacturers.

"Information about children often is used for marketing — to try to sell the kids things they don't need or the parents don't want to buy," she said. "The information can also be sold or shared with data brokers and can endanger a child's safety, especially if there's geolocation information, and it can be used to defraud or scam a family."

"Identity theft is so rampant in part because of data on the dark web. Even if the databases aren't shared, they're often hacked, and this is part of the reason that millions of people become victims of fraud and identity theft each and every year," Murray said.

This year's report highlighted Meta's new virtual reality (VR) headset, the Quest 3, and new VR accounts Meta offers to a target group of 10- to 12-year-old children.

"We found using Meta's new junior accounts greatly increases parental controls … but we also found these new additions fail to eliminate some real concerns," PIRG wrote.

"Playing games often requires agreeing to different third-party companies' data practices wholesale. VR headsets also can also gather sensitive motion data, which can be used to infer health or demographic details about you, and there's virtually no regulation controlling how companies or other actors use this data," according to PIRG.

Other identified risks involving Quest headsets included potential exposure to sexually graphic content and headsets "not designed to fit still-developing young bodies."

'Smart toys may potentially violate child privacy laws'

COPPA regulates online services targeted to children under age 13, including services that collect personal data. The law is enforced by the Federal Trade Commission (FTC).

Samuel Levine, director of the FTC's Bureau of Consumer Protection, told PIRG, "If the toy is directed to children under 13 years old … COPPA requires the toy company to ask for your consent before it collects your child's personal information.

But according to Gowda, "Smart toys may potentially violate child privacy laws."

In one example, Amazon faced charges from the FTC and U.S. Department of Justice (DOJ) earlier this year for COPPA violations stemming from allegations it illegally collected and used children's data collected via its Alexa-powered smart speakers.

Amazon "kept sensitive voice and geolocation data for years, and used it for its own purposes, while putting data at risk of harm from unnecessary access," the FTC found.

In July, Amazon reached a $25 million settlement and agreed to a permanent injunction requiring the company to "identify and delete inactive child profiles," and to "make disclosures" and avoid representations regarding "its retention and deletion practices regarding Alexa App geolocation information and voice information."

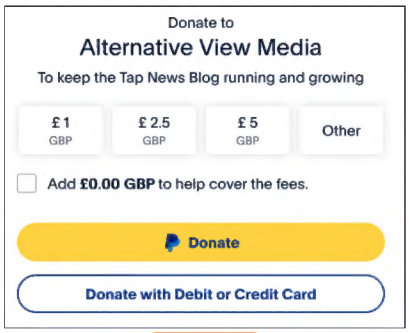
Another Big Tech company that recently ran afoul of COPPA is Microsoft, which faced accusations earlier this year that it collected information from Xbox users under 13 without notifying their parents.

Email Address

Subscribe

SUPPORT THE TAP

The Tap is managed and run by Alternative View Media. If you enjoy the Tap Blog then please show your support and help keep it online.



EVENTS COMING UP

The Alternative View Presents

Date: 24 March 2024

Time: 11:00 AM - 3:30 PM

Location: The Assembley Rooms, Glastonbury, UK

Tickets and Info

Join us for the first The Alternative View Presents with Gary Fraughen

Gary will be sharing his research and speaking about many subjects including:

Blue shift radiation
Super fluid consciousness with servants
Savants and greed
Numbers in the cracks and crevices of the universe
The universal balance sheet of doing harm to others

This is your opportunity to get up close and personal with Gary. This will be a more intimate event with plenty of opportunity for questions and discussion.

Tickets and info

ADVERTISMENTS

Loading

A Big Thank You

According to Murray, "The information included the children's first and last name, email address, date of birth and phone number. Microsoft had also sent the kids service agreements and advertising policies, and a pre-checked box allowing Microsoft to send promotional messages and to share user data with advertisers, Murray said.

In June, Microsoft agreed to pay a $20 million settlement and to make changes to its privacy protections for children.

Sheila Matthews, co-founder of AbleChild: Parents for Label and Drug Free Education, told The Defender that Xbox represents "a real concern," because "You can walk into a room and hear your child speaking to a stranger," she said. "You have no idea who that person is or how old that person is."

'Invasive and frightening' collection of biometric data

Joan Lawrence, senior vice president of standards and regulatory affairs and resident "Toy Safety Mom" at The Toy Association, a trade group representing U.S. toy manufacturers, retailers and licensors, told The Defender the toy industry strives to comply with all relevant privacy and child safety laws.

"Toy companies continually address emerging issues and challenges related to new technologies and prioritize the safety of children above all else," she said. "Responsible, legitimate toymakers follow guidance developed by the FTC and [COPPA] provisions."

"All toys sold in the U.S. are subject to more than 100 strict mandatory toy safety standards and tests," she added. "This applies to children's toys with or without a connected feature. Additionally, toys and children's products that have a connected feature are required to comply with the safeguards under COPPA."

Murray acknowledged that the toy industry holds itself to high standards and that the safety laws are robust. But "trying and doing are two different things," she said. "Large toy and product manufacturers in fact sometimes fail miserably, as we see in some of the cases brought by the FTC and DOJ in recent years."

"We're concerned the threats could escalate as artificial intelligence is used more, especially in toys." She referenced the FTC's settlement with Microsoft, which "makes clear that avatars generated from a child's image, and biometric and health information, are covered by [COPPA] when collected with other personal data."

According to the FTC, "biometric data" includes but is not limited to "eye tracking, iris and retina scans, voiceprint, scan and hand and face geometry, fingerprint, and gait," in addition to "physiological responses … and vital signs," reported PIRG.

"This strongly suggests the FTC is concerned that some companies can or will collect children's iris scans, fingerprints and vital signs and more," Murray said. "This is incredibly invasive and frightening."

"How could companies use this information in toys?" Murray continued. "AI is capable of processing children's facial expressions and determining when a child is happy or sad, or using children's voices to determine when a child is excited or scared."

Lawrence told The Defender the toy industry and the FTC have struck a balance.

"The FTC has recognized that when companies adopt careful procedures to manage voice recordings associated with voice-activated toys by promptly deleting the recording once the request has been recognized, they strike an appropriate balance of fostering an engaging experience while protecting children's privacy," she said.

Both PIRG and Murray called for stronger legislation to protect children's privacy, with PIRG also calling for stronger labeling standards for smart toys.

"Lawmakers should pass stronger data privacy laws, explicitly prohibiting companies from gathering more data from consumers than is necessary to deliver the service a consumer is expecting to get, and using it for any secondary purposes, especially for data that could be generated while using a VR headset," Murray said.

Murray said PIRG supports several bills in Congress that if passed, would improve protections for children's privacy.

"We support the bipartisan COPPA 2.0 … which updates the 1998 COPPA to better protect kids' and teens' privacy online, particularly regarding data collection, advertising and a parent's ability to delete their child's information on file," she said.

Murray said other proposed laws PIRG supports include the TOTS Act, which she said would require smart toy manufacturers to clearly label the package if the toy uses a Wi-Fi connection and collects children's data.

The Informing Consumers about Smart Devices Act would require manufacturers of household items to disclose, prior to purchase, if those products contain audio or visual recording components and can transmit data through Wi-Fi.

The Sunshine in Product Safety Act would enable the U.S. Consumer Product Safety Commission to warn consumers more quickly about dangers identified in consumer products, including toys, prior to a recall.

"Lawmakers should enforce current commerce laws and privacy laws not for big corporations but for families," Matthews said, adding that state lawmakers should also be pressured.

"The public health department in each state should be providing consumers with more information relating to informed consent and technology," she said, noting that AbleChild recently before Connecticut lawmakers regarding "children's jewelry coming in from China and the potential lead hazards."

"Our testimony focused on informed consent, making sure that parents were made aware of the metals that were compounded into the jewelry," she said. "This same informed consent applies to technology. Any third-party interaction with your children should be fully disclosed prior to purchase."

'Parents need to do more than read reviews'

A big thank you to those of you who attended the AV13 Conference in Milton Keynes. It was fantastic to finally get back together and welcome old friends and newcomers to a very enjoyable and memorable event. We are already already working on the next AV events.

If you didn't make it to AV13 we now have the presentation recordings available.

Regards and best wishes.

The AV Team.

www.alternativeview.co.uk

How to Watch

To watch please click on any video and purchase a ticket. Once you have made your purchase you will be sent an automatic email confirmation with your password details. You have unlimited viewings for the duration of your ticket.

Important: Please check your spam folder after your purchase as sometimes the confirmations go to spam. If you don't receive your password within 10 mins please contact us. We also have a help page. www.alternativeview.co.uk/help-page

RECENT POSTS

20 Amazing Artifacts at the Egyptian Museum.

So good they are. Recommend your friends now.

'Chilling': Some Smart Toys Can Collect Kids' Iris Scans, Fingerprints, Vital Signs and More

I wish to report a theft. Octopus Thieving Bastards steal £2000 from a positive balance.

If those "green" billionaires are so afraid of "global warming," why do they still own huge oceanside estates?

Is Mike Yeadon being Censored?

New Zealand Gov't Exempted Elite From 'Deadly' Covid Jabs, While Forcing Vax on Public

SHARING

RECENT COMMENTS

pete fairhurst 2 on New Zealand Gov't Exempted Elite From 'Deadly' Covid Jabs, While Forcing Vax on Public

ian on FBI Chief Warns Hamas-Inspired Terror Threats Have Reached Unprecedented Level

John on FBI Chief Warns Hamas-Inspired Terror Threats Have Reached Unprecedented Level

Belyi on Stay Free If You Lie. Prison if you tell the truth.

ian on New Zealand Gov't Exempted Elite From 'Deadly' Covid Jabs, While Forcing Vax on Public

Tapestry on Mathis the scientist

ian on Stay Free If You Lie. Prison if you tell the truth.

ATOM FEED

The PIRG report — and experts who spoke with The Defender — said parents should be more proactive in researching the toys they are considering purchasing and familiarizing themselves with the capabilities of toys they have already purchased.

"Parents whose children already have smart toys should go back and read the privacy policies, either that came with the toy or online," Murray said.

"Yes, the language can be dense," she added. "It's important to learn what information the companies are collecting, what information it has already collected that you can review and what information about your child that you want deleted."

If they already own toys that can track or communicate with their children and they are not sure, AbleChild suggests parents research the capabilities of the toy and limit the exposure, Matthews said.

PIRG recommended parents perform an online search on all toys they are considering purchasing and familiarize themselves with the features built into the toys, including any internet, Wi-Fi, Bluetooth or social media connections and any data-collection and storage capabilities the toy may have.

This includes finding out about any audio or video recording capabilities or email and messaging capabilities the toy may potentially have, PIRG noted.

"Parents need to do more than read reviews on Amazon," Matthews said. "They should investigate the actual toy, where it is made, what the capabilities are, and will it benefit my child's development."

Lawrence recommended reading toys' privacy policies, enabling all parental controls, disabling cameras and chat functionalities, turning off location services on devices, activating two-step verification to protect online accounts, and securing home Wi-Fi networks. If a toy is passed on to others, "reset it to clear its memory," she said.

"Parents should also review how to 'turn off' the smart features when they're not needed. If they can't be turned off, then maybe the toy needs to be unplugged or have the batteries removed. Or you might want to take it to your garage or vehicle when it's not in use," Murray said, adding that communication with children is also important.

"Parents should also consider having age-appropriate conversations with their kids about what information is okay to share or not, even with a toy, much like how we were all warned as young children about not getting into a car with a stranger," she added.

"Starting when your child is young, explain to them the importance of never giving out their personal information to people online, and teach them how to create strong passwords — and change them regularly," Lawrence said.

This year's "Trouble in Toyland" report also highlighted risks from low-tech toys such as water beads, button batteries, and counterfeit and recalled toys. In the report, Murray said 150,000 children are treated in emergency rooms annually with toy-related injuries.

"Water beads should not be purchased as a toy. Full stop. They're dangerous. They expand when put in water, from perhaps the size of a pea to the size of a golf ball," Murray said, noting that such toys, if swallowed, expand in the child's esophagus and digestive tract, with the risk of blocking airways and causing an intestinal obstruction.

"Parents with younger children should also periodically check their children's toys and make sure that those played with a lot haven't started wearing out to the point that they have loose parts or other issues that could be a risk," Murray said."

Source: https://childrenshealthdefense.org/defender/smart-toys-biometric-data-collection-children/

Post Views: 15

LEAVE A REPLY

You must be logged in to post a comment.

This site is intended as an informational guide. The remedies approaches and techniques described hearin are meant to supplement, and not be a substitute for, professional, medical care or treatments. Any information is for entertainment purposes only. Any previous articles which prefix the **8th of February 2023** have no involvement in new upload to this site. Any Copy right infringements are not intended and any such should be made aware to the site for immediate withdraw. Articles posted here are for your consideration at your discretion. No purported facts have been verified. Articles do not necessarily reflect the views of the poster nor the site owner.

Blog editor - editor[at]tapnewswire.com